## COMPLETE LISTING OF THE CLAIMS

The following lists all of the claims that are or were in the above-identified patent application. The status identifiers respectively provided in parentheses following the claim numbers indicate the current statuses of the claims.

1. (Currently Amended) A method of enabling a second party to prove to a third party the existence of an association between the second party and a first party, the first party being associated with a first element of a first algebraic group, the second party being associated with a second element, of a second algebraic group, formed from an identifier string of the second party using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party:

receives a shared secret provided by the first party as the product of a first secret and the second element;

computes first, second and third verification parameters, wherein ~~as~~ the first verification parameter is a product of a second secret ~~with, respectively,~~ and said shared secret, the second verification parameter is a product of the second secret and the second element and the third verification parameter is a product of the second secret and the first element; and

outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties.

2. (Previously presented) A method according to claim 1, wherein the second-party computer entity generates a further shared secret from the second secret and an identifier string of a fourth party, the second party outputting this further shared secret to the fourth party for use by the latter as the private key of a public/private key pair the public key of which is formed by the identifier string of the fourth party.

3. (Original) A method according to claim 1, wherein the first and second parties are respectively parent and child trusted authorities in a hierarchy of trusted authorities.

PATENT LAW OFFICE OF DAVID MILLER
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

4. (Original) A method according to claim 1, wherein the first and second algebraic groups are the same.

5. (Original) A method according to claim 1, wherein the first and second elements are points on the same elliptic curve.

6. (Previously Presented) A method of verifying an association between the first and second parties of claim 1 by using a function $p$ providing said bilinear map; the method comprising a third-party computer entity carrying out the following operations using the verification parameters of claim 1:

computing the second element from the identifier string of the second party;

carrying out a first check to determine that the following equality is satisfied:

$p$(third verification parameter, computed second element)

$= p$(first element, second verification parameter)

carrying out a second check to determine that the following equality is satisfied:

$p$(first element, first verification parameter)

$= p$(first product, second verification parameter) where said first product is a public parameter provided by the first party and corresponds to the product of the first secret and the first element;

verifying the existence of the association between the first and second parties only where checks are passed.

7. (Original) A method according to claim 6, wherein said bilinear mapping function is based on a Tate or Weil pairing.

8. (Previously Presented) A method of verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group, the first and second elements being such that there exists a bilinear mapping p for these elements, the method comprising a third-party computer entity carrying out the following operations:

receiving both data indicative of said first element, and a first product formed by the first party from a first secret and the first element;

PATENT LAW OFFICE OF
DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

receiving in respect of the second party an identifier string and first, second and third verification parameters;

computing the second element from the identifier string of the second party;

carrying out a first check to determine that the following equality is satisfied:

$p$(third verification parameter, computed second element) = $p$(first element, second verification parameter)

carrying out a second check to determine that the following equality is satisfied:

$p$(first element, first verification parameter)= $p$(first product, second verification parameter)

verifying the existence of the association between the first and second parties only where checks are passed.

9. (Original) A method according to claim 8, wherein said bilinear mapping function is based on a Tate or Weil pairing.

10. (Original) A method according to claim 8, wherein the first and second algebraic groups are the same.

11. (Original) A method according to claim 8, wherein the first and second elements are points on the same elliptic curve.

Claims 12 - 18. Cancelled.

19. (Currently Amended) Apparatus arranged to enable a third party to verify an association between the apparatus and a first party that has a first secret and is associated with a first element of a first algebraic group, the apparatus being associated with a second element, of a second algebraic group, and the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

a memory for holding a second secret and an identifier string associated with the apparatus,

means for forming said second element from said identifier string using a hash function,

PATENT LAW OFFICE OF DAVID MILLER
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

means for receiving from the first party a shared secret based on said first secret and said first element, and for storing this shared secret in the memory,

means for computing first, second and third verification parameters, wherein ~~as~~ the first verification parameter is a product of the second secret with said shared secret, the second verification parameter is a product of the second secret and said second element and the third verification parameter is a product of the second secret and said first element ~~respectively~~, and

means for making available said identifier string and said verification parameters to the third party.

20. (Original) Apparatus according to claim 19, wherein the first and second algebraic groups are the same.

21. (Original) A method according to claim 19, wherein the first and second elements are points on the same elliptic curve.

22. (Previously Presented) Apparatus for verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group; the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

means for receiving both data indicative of the first element, and a first product formed by the first party from a first secret and the first element;

means for receiving in respect of the second party both an identifier string, and first, second and third verification parameters;

means for computing the second element from the identifier string of the second party using a hash function;

means for carrying out a first check to determine that the following equality is satisfied:

$p$(third verification parameter, computed second element) = $p$(first element, second verification parameter);

means for carrying out a second check to determine that the following equality is satisfied:

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

$p$(first element, first verification parameter) = $p$(first product, second verification parameter);

means responsive to both checks being passed, to confirm that there exists an association between the first and second parties.

23. (Original) Apparatus according to claim 22, wherein said bilinear mapping p is based on a Tate or Weil pairing.

24. (Original) Apparatus according to claim 22, wherein the first and second elements are points on the same elliptic curve.

Claims 25–28 (Cancelled)

29. (Previously Presented) A method of enabling a second party to prove to a third party the existence of an association between the second party and a first party, the first party being associated with a first element of a first algebraic group, the second party being associated with a second element, of a second algebraic group, formed from an identifier string of the second party using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party:

(1) receives a shared secret provided by the first party as the product of a first secret and the second element;

(2) computes:

(i) a first verification parameter as the product of a second secret with said shared secret,

(ii) a second verification parameter as the product of the second secret with the second element, and

(iii) a third verification parameter as the product of the second secret with the first element; and

(3) outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties.

PATENT LAW OFFICE OF
DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543